

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re application of:

Roger D. Pirkey et al.

Confirmation No. 1489

Serial No.: 09/732,333

Examiner: Pyzocha, Michael J.

Art Unit: 2137

Filed: December 6, 2000

Atty. Docket No. 010942-0269227

AWT-002

For: Enhanced PIN-Based Security Method and Apparatus

---

Submitted electronically via EFS on August 14, 2007.

**CORRECTED APPEAL BRIEF**

Mail Stop APPEAL

Commissioner for Patents

P.O. Box 1450

Alexandria, VA 22313-1450

Sir:

This paper is further to the Notice of Appeal filed February 17, 2007, and the Panel Decision from Pre-Appeal Brief Review mailed March 9, 2007. A supportive brief was originally filed April 16, 2007.

This paper is also in response to the Notice of Non-Compliant Appeal Brief mailed July 17, 2007, for which a response is due August 17, 2007. Appellants claim small entity status, see 37 CFR 1.27. The Commissioner is authorized to charge any required fee to Pillsbury Winthrop Shaw Pittman LLP's deposit account no. 50-2213 (order no. 010942-0269227).

### ***REAL PARTY IN INTEREST***

The real party in interest is Aurora Wireless Technologies, Ltd., which has full title to the present application by virtue of an assignment from the inventors recorded at Reel/Frame No. 011879/0463.

### ***RELATED APPEALS AND INTERFERENCES***

There are no appeals or interferences that will directly affect, be directly affected by, or have a bearing on the Board's decision in this appeal.

### ***STATUS OF CLAIMS***

Claims 1, 2, 4-6, 9, 11-13, 16, 17, 19-21, 24, 26-28 and 31-42 are pending in the application, all of which stand finally rejected. Claims 3, 7, 8, 10, 14, 15, 18, 22, 23, 25, 29, 30 have been canceled. The rejections of all pending claims 1, 2, 4-6, 9, 11-13, 16, 17, 19-21, 24, 26-28 and 31-42 are appealed.

### ***STATUS OF AMENDMENTS***

In response to the Final Office Action mailed December 21, 2006, Appellants filed a request for reconsideration on January 8, 2007. This response did not include any amendments and was not deemed to place the application in condition for allowance (Advisory Action mailed January 22, 2007). No further amendments have been filed and not entered.

### ***SUMMARY OF CLAIMED SUBJECT MATTER***

The present invention provides a method and apparatus that reduces fraudulent or unauthorized use of resources in a network such as a cellular phone network, while minimizing unnecessary inconvenience to network subscribers.

In accordance with certain aspects, the invention includes a novel validation process (e.g. 212 in FIG. 2) and profiling database (e.g. 124 in FIG. 1). The profiling database contains several "system wide" lists of resources such as phone numbers. In a phone network example, these lists define which numbers cannot be called from any mobile sets operating in the network.

The lists may also define which numbers can be called by any subscriber without using a personal identification number (PIN) (e.g. emergency calls such as to 911 or 0) and which numbers always require a PIN (e.g. 900 number calls).

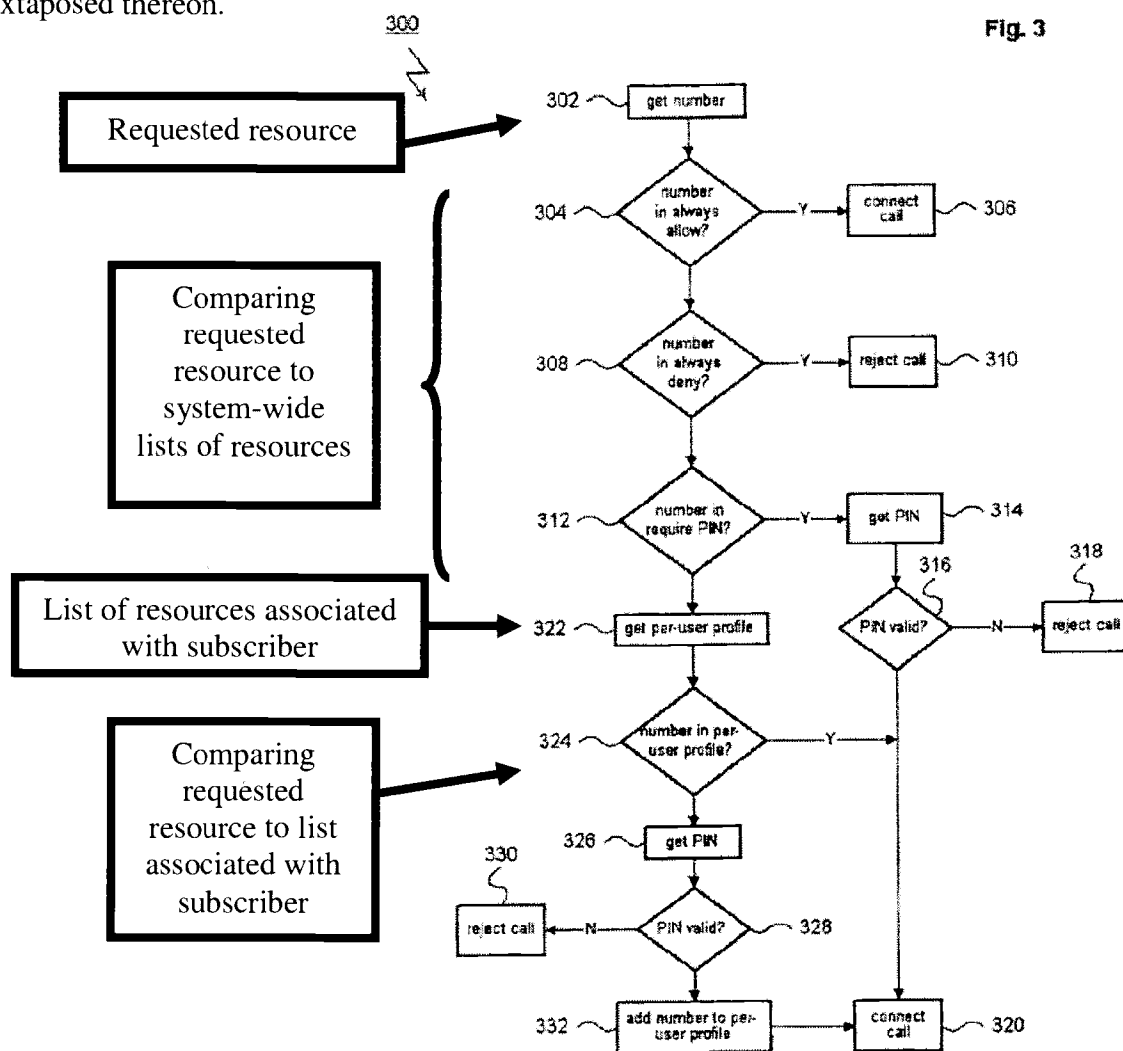
In addition to the “system wide” lists, the profiling database stores an individual subscriber profile for each subscriber. In one phone network example, each individual subscriber profile lists the phone numbers that its associated subscriber may dial without using a PIN. In such an example, when a subscriber dials a number that is not included in their individual subscriber profile, a PIN is required by the validation process. If the PIN is correctly entered, the phone call is allowed and the number is added to the subscriber's individual subscriber profile by the validation process. (see, e.g. page 3, line 27 to page 4, line 7 of the present specification)

According to further aspects of the invention, the system-wide lists (e.g., Always require PIN list, Always allow list, Always deny list) take precedence over the individual subscriber profiles. For example, a system-wide list of phone numbers can provide the final determination as to whether a number can be dialed and whether the number requires a PIN.

More particularly, as shown and described in connection with FIG. 3, an example embodiment of the inventive method which can be included in validation process 212 is invoked by a call originated by a subscriber using one of mobile stations 102. Validation process 212 begins by retrieving the number being dialed. First, validation process 212 consults several different system-wide lists of resources to determine if the number being called is present in the those lists (e.g. always allow list in step 306, always deny list in step 308, always require PIN list in step 312) of profiling database 124. If the number is in one or more of the system-wide lists, the call is handled accordingly.

If the number is not on any of the system-wide lists, validation process 212 retrieves the individual subscriber profile associated with the subscriber placing the call, and in step 324, validation process 212 consults the just-retrieved individual subscriber profile to determine if the number being called is present. If the number being called is included in the subscriber's individual subscriber profile, validation process 212 allows the call to complete. Otherwise, validation process 212 retrieves a PIN from the subscriber making the call, and accepts or rejects the call based on whether the supplied PIN is valid.

For convenience, FIG. 3 is reproduced below, with terminology from the claims juxtaposed thereon.



Accordingly, each independent claim (claims 1, 9, 16 and 24) of the present application specifically requires maintaining separate lists of resources (e.g. phone numbers). A “system wide” list specifies resources (e.g. phone numbers) to which access is controlled regardless of the identity of the subscriber. When a subscriber requests access to a resource (e.g. requesting a connection to a destination phone number), the requested resource is first compared to the “system wide” list. If the resource is not on the “system wide” list, a list specifically associated with the subscriber is then retrieved. If the resource is not on the subscriber’s own list either, the

subscriber must enter a PIN to access the resource. (see FIG. 3, page 3 line 27 to page 4 line 7, for example).

More particularly, independent claim 1 sets forth a method that clearly requires “concurrently maintaining” separate lists of resources (e.g. phone numbers). A “system wide” list specifies resources (e.g. phone numbers) to which access is controlled regardless of the identity of the subscriber. The method further requires that when a subscriber requests access to a resource (e.g. requesting a connection to a destination phone number), the requested resource is first compared to the “system wide” list. If the resource is not on the “system wide” list, a list specifically associated with the subscriber is then retrieved. If the resource is not on the subscriber’s own list either, the subscriber must enter a PIN to access the resource. (see FIG. 3, page 3 line 27 to page 4 line 7, for example).

Further, independent claim 9 sets forth a method that clearly requires “maintaining” a first list of resources (e.g. phone numbers) and a “separate” second list of resources to which access is controlled regardless of the identity of the subscriber. The method further requires that when a subscriber requests access to a resource (e.g. requesting a connection to a destination phone number), the requested resource is first compared to the second (i.e. system wide) list. If the resource is not on the second (i.e. system wide) list, a list specifically associated with the subscriber is then consulted. If the resource is not on the subscriber’s own list either, the subscriber must enter a PIN to access the resource. (see FIG. 3, page 3 line 27 to page 4 line 7, for example).

Independent claim 16 sets forth an apparatus that clearly requires “means for concurrently maintaining” separate lists of resources (e.g. phone numbers) (e.g. profiling database 124 in Fig. 1). A “system wide” list specifies resources (e.g. phone numbers) to which access is controlled regardless of the identity of the subscriber. The apparatus further requires means for, when a subscriber requests access to a resource (e.g. requesting a connection to a destination phone number), the requested resource is first compared to the “system wide” list (e.g. validation process 212 in Fig. 2). If the resource is not on the “system wide” list, a list specifically associated with the subscriber is then retrieved. If the resource is not on the subscriber’s own list either, the subscriber must enter a PIN to access the resource. (see FIG. 3, page 3 line 27 to page 4 line 7, for example).

Finally, independent claim 24 sets forth an apparatus that clearly requires “means for maintaining” a first list of resources (e.g. phone numbers) and means for maintaining a “separate” second list of resources to which access is controlled regardless of the identity of the subscriber (e.g. profiling database 124 in Fig. 1). The apparatus further requires means for, when a subscriber requests access to a resource (e.g. requesting a connection to a destination phone number), the requested resource is first compared to the second (i.e. system wide) list. If the resource is not on the second (i.e. system wide) list, a list specifically associated with the subscriber is then consulted (e.g. validation process 212 in Fig. 2). If the resource is not on the subscriber’s own list either, the subscriber must enter a PIN to access the resource. (see FIG. 3, page 3 line 27 to page 4 line 7, for example).

### ***GROUND OF REJECTION TO BE REVIEWED ON APPEAL***

Claims 1-2, 4, 6, 9, 11, 13, 16-17, 19, 21, 24, 26 and 28 stand rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,134,447 to Havinis et al. (“Havinis”) in view of U.S. Patent No. 5,737,701 to Rosenthal et al. (“Rosenthal”). Claims 5, 12, 20, 27, 33, 36, 39, and 42 stand rejected under 35 U.S.C. 103(a) as being allegedly unpatentable over Havinis and Rosenthal in view of U.S. Patent No. 6,330,311 Mijares et al. (“Mijares”). Claims 31, 34, 37, and 40 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Havinis and Rosenthal in view of Rowell et al, WO 9704602 (“Rowell”). Claims 32, 35, 38, and 41 stand rejected as being unpatentable over Havinis and Rosenthal in view of Rudokas, US Patent 5,420,910 (“Rudokas”).

Appellants respectfully submit that these rejections are in error for multiple reasons, and seek review of them on the following reversible grounds:

- Whether the cited prior art, alone or in combination, teach or suggest the following claim limitations of each independent claim:
  - maintaining separate and distinct lists of resources, at least one listing resources to which access is controlled regardless of subscriber identity (i.e. “system-wide” list of resources), and at least one listing resources specifically associated with subscribers (i.e. “subscriber-specific” list of resources);
  - first determining whether to grant access by comparing a requested resource to the system-wide list of resources before comparing the requested resource to the subscriber-specific list of resources; and

- requiring a personal identification number (PIN) to be entered if the requested resource is not on either list.

### ***ARGUMENT***

The present claims patentably define over the cited prior art at least because the references, alone or in combination, do not teach or suggest all the limitations of the claims. Meanwhile, the Federal Circuit requires that “[a]ll words in a claim must be considered in judging the patentability of that claim against the prior art.” In re Wilson, 424 F.2d 1382, 1385 (CCPA 1970). Accordingly, the Examiner has failed to establish a prima facie case of obviousness and the § 103 rejections of the claims should be reversed for at least this reason. See MPEP 2143.03. Moreover, even if, arguendo, all claim limitations were suggested, at best it would have only been obvious to try to combine the cited references. And finally, even if one skilled in the art would combine the references in a manner suggested by the Examiner, their principles of operation would be completely changed. Accordingly, the cited prior art can not establish a prima facie case of obviousness for this additional reason. See MPEP 2143.01.

### **The Cited Prior Art Does Not Support A Prima Facie Case Of Obviousness Because Alone Or In Combination, They Do Not Teach Or Suggest Maintaining And Using Two Different Types of Lists of Resources As Defined By The Claims**

Independent claims 1, 9, 16 and 24 require, inter alia:

1. Maintaining a “system-wide” list of resources to which access can be controlled without reference to a subscriber’s identity;
2. Concurrently maintaining a plurality of separate and distinct lists of resources to which access is controlled specifically in accordance with a respective subscriber’s identity;
3. First comparing a requested resource to the “system-wide” list to determine whether access to the resource should be provided;
4. If the resource is not on the “system-wide” list, retrieving a list of resources specific for the requesting user; and
5. Requiring a PIN to be entered if the requested resource is not on the user’s specific list.

The Examiner alleges that the invention of the independent claims is suggested by the alleged combination of Havinis and Rosenthal. For convenience, the text of claim 1 is reproduced below, along with the Examiner's allegations regarding Havinis and Rosenthal.

<b>Claim 1</b>	<b>Havinis</b>	<b>Rosenthal</b>
A method for providing access to resources with the use of personal identification numbers, comprising the steps of:	<p>"A telecommunications system and method is disclosed for administration of location services by using black and gray location application lists within a positioning gateway. When a location application subscribes to location services, the wireless service provider assigns a unique Location Application Identifier Number (LAIN) to the location application, which is included in every positioning request. The black list is used to bar service to the location applications included in the list, while maintaining the location application's location application profile in the positioning gateway. Location applications included in the gray list are not barred from service, but instead are monitored by the wireless operator." (Abstract)</p>	<p>"A communications system is designed to exempt communications services users, such as wireless communications subscribers and calling card callers, from entering an authentication code for calls directed to pre-selected destination numbers, notwithstanding the authentication code entry requirement implemented by the communications services provider for all other calls." (Abstract)</p>
concurrently maintaining a system-wide list of resources associated with a plurality of subscribers regardless of subscriber identity and a separate and distinct plurality of lists of resources respectively associated with subscribers;	<p>Havinis maintains a "Black" list of LAINs (i.e. subscriber identities) and a "Gray" list of LAINs (i.e. subscriber identities) (Abstract)</p>	<p>Rosenthal maintains a plurality of lists of phone numbers (i.e. resources) specifically associated with a plurality of subscribers. (Fig. 3)</p> <p>Rosenthal admittedly does not teach or suggest a "system-wide" list</p>



<b>Claim 1</b>	<b>Havinis</b>	<b>Rosenthal</b>
receiving a request from a subscriber to access a resource;	Havinis's system receives requests by LA's (i.e. subscribers) for location services (i.e. resource) (Fig. 4, box 400)	Rosenthal's system receives requests from subscribers to dial a telephone number (i.e. resource) (Fig. 4, box 401)
first comparing the resource to the system-wide list;	Havinis first compares the requesting LA's identity to a "Black" list of subscriber identities who are always barred from accessing location services (Fig. 4, box 405)	Rosenthal admittedly does not teach or suggest a "system-wide" list
if the resource is included in the system-wide list: providing or denying access to the resource in accordance with the system-wide list;	Havinis denies service to the requesting LA if its LAIN (i.e. subscriber identity) matches one in the "Black" list (Fig. 4, box 420)	Rosenthal admittedly does not teach or suggest a "system-wide" list
if the resource is not included in the system-wide list: retrieving one of the plurality of lists associated with the subscriber;	Havinis next checks a single "Gray" list if the LA's identity was not in the "Black" list (Fig. 4, box 410)	Rosenthal always retrieves the subscriber-specific list when an authentication code is not provided (Fig. 4, box 405)
next comparing the resource to the retrieved list associated with the subscriber;	Havinis compares the requesting LA's identity to a "Gray" list of subscriber identities whose access should be monitored (Fig. 4, box 410)	Rosenthal only compares the requested phone number to the numbers in the subscriber's own lookup table (Fig. 4, box 407)
providing access to the resource if the resource is included in the list associated with the subscriber; requiring the subscriber to input a personal identification number if the resource is not included in the list associated with the subscriber; and providing access to the resource if the subscriber inputs the correct personal	Havinis monitors the location service if the LA's identity was in the "Gray" list (Fig. 4, box 425, Abstract)	Rosenthal requires authentication if the requested phone number is NOT in the subscriber's list (Fig. 4, box 411)  Rosenthal allows access to the requested phone number without authentication if the phone number is in the subscriber's list (Fig. 4, box 409).

<b>Claim 1</b>	<b>Havinis</b>	<b>Rosenthal</b>
identification number.		

Neither Havinis Nor Rosenthal Teaches Or Suggest Two Different Lists of Resources As Defined By The Claims

The Examiner admits that Rosenthal does not suggest two different lists of resources, and as shown above, at most it only suggests a plurality of user-specific lists of resources. Accordingly, the Examiner relies on Havinis as teaching two different lists of resources. As stated in the Advisory Action:

Havinis was relied on to teach the use of two lists (one system-wide and one with respect to individual subscribers) and checking these lists in a specific order and performing actions based on these lists.

However, neither of Havinis's "two lists" contains resources, and neither is a "system-wide" list per the claims.<sup>1</sup> The Office Action identifies Havinis's "black list 392" and "gray list 394" as the alleged "two lists." But both of these are lists of LAIN's, or identities of subscribing LA's, not resources. Moreover, they are both specific to the identities of LA's, contrary to the Examiner's statement in the Advisory Action, and so cannot possibly be a "system-wide" list per the claims. More particularly, the "black list 392" contains identities of subscribing LA's that are always denied access to location services (e.g. identities of subscribers who have not paid their bill) (col. 3, lines 47-49; col. 5, lines 4-14). The "gray list 394" contains identities of subscribing LA's whose access to location services should be monitored. (col. 3, lines 49-51; col. 5, lines 32-44)

Clearly, neither of Havinis' lists are lists of resources, much less a "system-wide" list of resources to which access may be controlled without considering the identity of the requesting subscriber, nor a distinct plurality of lists associated with specific subscribers, as required by the claims.

---

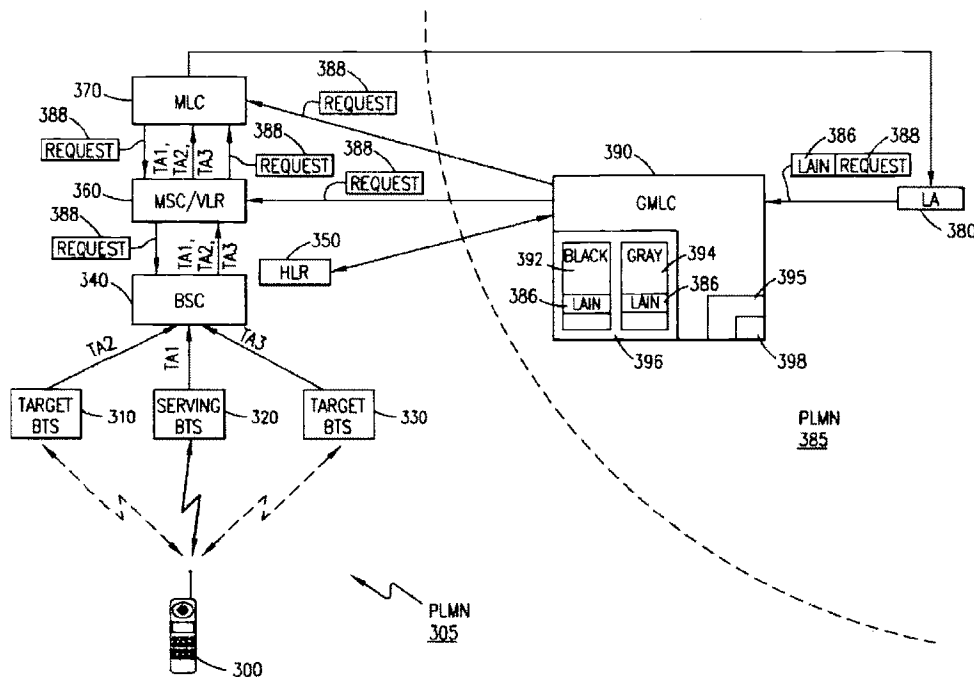
<sup>1</sup> The Examiner, in the Advisory Action, argues that one "cannot show nonobviousness by attacking references individually." Appellants agree, but it is the Examiner who is relying on Havinis as suggesting the two types of lists in the claims. Appellants are merely responding to this specific allegation by the Examiner regarding Havinis' individual teachings.

Havinis's LA's Are Subscribers, So Havinis's "Black List" Is Not A "System-Wide List of Resources" Merely Because LA's Are Associated With Groups of Cell Phones

Despite the undeniable fact that Havinis's "two lists" are both lists of LAIN's -- i.e. lists containing identities of specific subscribing LA's -- the Advisory Action takes the further position that they are both "system-wide" lists because "the location application 'is associated with a group of subscribers.'" However, this position contradicts the Examiner's earlier statement that Havinis teaches two different types of lists. In other words, since both the "black" and "gray" lists clearly both contain identities of LA's, one cannot be a "system-wide" list while the other is not. Accordingly, for this reason alone the rejections should be reversed.

In any event, this contradictory position mischaracterizes Havinis's teachings. Havinis discloses only one type of subscriber for whom access to location services can be controlled: location applications (LA's). Although multiple cell phones can be associated with a given location application (LA), the location applications (LA's) are clearly subscribers, and not resources.<sup>2</sup>

More particularly, Havinis uses the term "location application" to correspond to an organization that has a subscription for receiving location services. For example, Havinis teaches that "[w]hen a location application (LA) subscribes to location services, the wireless service provider assigns a unique Location Application Identifier Number (LAIN) to the LA. . . ." (col. 3, lines 43-46, emphasis added) Examples of LA's taught by Havinis include emergency centers, law enforcement agencies and fleet management companies. (col. 4, lines 30-40)



With reference to FIG. 3 from Havinis reproduced above, in Havinis's system, the LA 380 (e.g. a fleet management company) subscribes to and requests location services for locating phones such as 300 that are associated with the LA. As further shown above, these requests 388 include the LA's subscription identity (LAIN) 386. This subscriber identity is compared to a list (i.e. black list 392) of subscriber identities to determine whether to perform the requested location service.

Although Havinis teaches that an LA can be associated with a group of cell phone subscribers, at best this means that Havinis associates one type of subscriber (i.e. multiple cell phones) with another type of subscriber (i.e. single location application (LA)). This does not mean the black list does not contain identities of subscribers. There can simply be no question that lists 392 and 394 contain identities (i.e. LAINs) of subscribers (i.e. LA's). In fact, the Advisory Action admits that "the black lists are checked using the LAIN" (i.e. LA identifier number). Because the LAIN is clearly the identity of a subscriber (i.e. a subscribing LA) to location services, just because the black list does not contain identities of cell phones does not mean it does not contain any identities. Rather, as the Advisory Action admits, Havinis teaches that the black (and gray) list contains identities of specific subscribing location applications.

<sup>2</sup> Thus, while Havinis' use of the term "application" in the term "location application" (LA) is somewhat

### Havinis and Rosenthal Combined Do Not Suggest The Claimed Lists of Resources

The Advisory Action further takes the position that because Havinis teaches “two lists” and Rosenthal teaches a “list of resources,” the alleged combination of Havinis and Rosenthal “teaches the claimed limitations.” In this manner, the Advisory Action appears to concede that Havinis’s lists do not contain lists of resources. However, the Advisory Action apparently takes the position that Havinis teaches a “system-wide” list, which combined with Rosenthal’s alleged “list of resources,” together suggest a “system-wide list of resources.”

This position is wrong in both law and fact. First, it is respectfully submitted that the Examiner is improperly plucking and choosing words and fitting them together using the claim language as a roadmap.

In any event, this position is factually incorrect because neither Havinis nor Rosenthal teaches or suggests the claimed “system-wide list of resources,” to which access is controlled regardless of the identity of the requesting subscriber. Clearly, both Havinis’s “black” and “gray” lists and Rosenthal’s profiles explicitly depend on and control access to resources based on the identity of the requesting subscriber. In Havinis, the subscribing LA’s identifier (LAIN) is compared to the “black” and “gray” lists of LAINs. In Rosenthal, the subscriber’s identity is used to retrieve the subscriber’s own lookup table of destination phone numbers. Clearly, neither reference teaches or suggests a “system-wide list of resources associated with a plurality of subscribers” that is used to control access to resources regardless of the identity of the requesting subscriber as explicitly required by the claims.

Accordingly, because the cited prior art does not teach or suggest all claim limitations, they do not establish a prima facie case of obviousness and the rejections should be reversed.

### **The Prior Art Fails To Support A Prima Facie Case Of Obviousness Because At Best It Would Only Have Been Obvious To Try To Combine The Cited References**

Havinis teaches a system that allows organizations to locate cell phones, and aims at reducing fraud by allowing certain of these organizations to be “black” listed or “gray” listed

---

misleading, Havinis itself makes it explicitly clear that LA’s are subscribers for location services.

from receiving location services. Rosenthal merely teaches an automatic authentication system using PINs for a phone system.

The Office Action alleges that one skilled in the art would have been motivated to combine Rosenthal's use of PINs in Havinis's system "to help prevent fraud in the system." However, Havinis's system already aims at preventing fraud in location services by using black lists and gray lists. Meanwhile, Rosenthal aims at controlling access to phone service using PINs. Both are entirely different approaches, and both are aimed at completely and fully solving the different problems confronted in the respective environments.

There is no teaching or suggestion in Havinis or Rosenthal that their own solutions are insufficient for solving the problems they address. Put another way, one skilled in the art would not read Havinis and Rosenthal to mean that they are alone incapable of preventing fraud in their respective environments. Accordingly, at best it would be obvious to try combining the two different approaches in one, even assuming arguendo that doing so would meet all the claim limitations. Moreover, it is believed that only impermissible hindsight using the claimed invention as a roadmap would lead one to combine the two references in a manner suggested by the Office Action.

Accordingly, the cited prior art does not support a prima facie case and the rejections should be reversed for this additional reason.

**The Prior Art Fails To Support A Prima Facie Case Of Obviousness Because If Combined In A Manner To Meet The Claim Language, Their Principle Of Operation Would Be Changed**

Havinis teaches a system that allows organizations to locate cell phones, and enables certain of these organizations to be "black" listed or "gray" listed from receiving location services. Rosenthal teaches an automatic authentication system for use in a phone system.

Combined together, the Examiner's hypothetical system would include Havinis's subscriber-specific black and gray lists and Rosenthal's subscriber-specific individual lookup tables. Conceivably, this hypothetical system might first check the subscriber's identity to determine whether the requesting subscriber is "black" or "gray" listed, and then check the

subscriber's own profile to determine whether the destination phone number is in the lookup table.<sup>3</sup>

As such, this hypothetical system would not suggest the invention because, as set forth above, there is no "system-wide list of resources" to which access is controlled regardless of the identity of the requesting subscriber.

In order to meet the limitations of the claims, one skilled in the art would have to modify this hypothetical system such that Havinis's "black" or "gray" list of subscribers instead contain lists of resources to which access should be controlled. But this would fly in the face of Havinis's teachings. Havinis is aimed at controlling access to one resource (i.e. location services), and merely allows for certain requesting subscribers to be black listed or gray listed, for example because they have "not paid [their] location services bill." (col. 5, lines 5-6) Accordingly, by changing Havinis's teachings to meet the claim language, Havinis's entire scheme of operation and objective of barring resources to non-paying subscribers would be changed. Meanwhile, courts have held that if the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims prima facie obvious. In re Ratti, 270 F.2d 810 (CCPA 1959).

Accordingly, the cited prior art does not support a prima facie case and the rejections should be reversed for this additional reason.

---

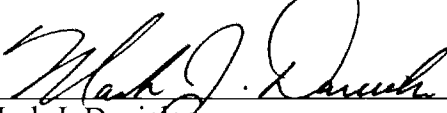
<sup>3</sup> This combination and progression is not suggested by either reference, but is presented here for sake of argument.

***CONCLUSION***

For the foregoing reasons, Appellants respectfully request that all the pending claims be deemed allowable by this honorable Board.

Respectfully submitted,  
PILLSBURY WINTHROP SHAW PITTMAN LLP

Date: August 14, 2007



Mark J. Danielson

40,580

Reg. No.

Telephone: (650) 233-4777

Facsimile: (650) 233-4545

Please reply to customer no. 27,498



## CLAIMS APPENDIX

1. (Previously Presented) A method for providing access to resources with the use of personal identification numbers, comprising the steps of:
  - concurrently maintaining a system-wide list of resources associated with a plurality of subscribers regardless of subscriber identity and a separate and distinct plurality of lists of resources respectively associated with subscribers;
  - receiving a request from a subscriber to access a resource;
  - first comparing the resource to the system-wide list;
  - if the resource is included in the system-wide list:
    - providing or denying access to the resource in accordance with the system-wide list;
  - if the resource is not included in the system-wide list:
    - retrieving one of the plurality of lists associated with the subscriber;
    - next comparing the resource to the retrieved list associated with the subscriber;
    - providing access to the resource if the resource is included in the list associated with the subscriber;
    - requiring the subscriber to input a personal identification number if the resource is not included in the list associated with the subscriber; and
    - providing access to the resource if the subscriber inputs the correct personal identification number.
2. (Original) A method as recited in claim 1 further comprising the step of adding the resource to the list associated with the subscriber if the subscriber inputs the correct personal identification number.
3. (Canceled)

4. (Previously presented) A method as recited in claim 1 wherein the system-wide list includes an always deny list, and wherein the step of providing or denying access includes denying access to the resource if the resource is included in the always deny list.
5. (Previously presented) A method as recited in claim 1 wherein the system-wide list includes an always require PIN list, and wherein the step of providing or denying access includes requiring the subscriber to input a personal identification number if the resource is included in the always require PIN list.
6. (Original) A method as recited in claim 1 wherein the resource is a telephone connection to a destination phone number.
- 7-8. (Canceled)
9. (Previously presented) A method for providing access to resources with the use of personal identification numbers, comprising the steps of:
- maintaining a first list of resources accessed by a user;
  - maintaining a second list of resources separate from the first list, the second list listing resources to which access is controlled regardless of user identity;
  - first determining whether to allow the user to access resources included in the second list before consulting the resources in the first list;
  - requiring the user to enter a personal identification number to access a further resource not included in the first or second lists; and
  - adding the further resource that the user accesses using the personal identification number to the first list.
10. (Canceled)

11. (Previously presented) A method as recited in claim 9 wherein the second list includes an always deny list and wherein the first determining step includes denying the user access to a still further resource if the still further resource is included in the always deny list.

12. (Previously presented) A method as recited in claim 9 wherein the second list includes an always require PIN list and wherein the first determining step includes requiring the user to input a personal identification number to access a still further resource included in the always require PIN list.

13. (Original) A method as recited in claim 9 wherein the resources are telephone connections to destination phone numbers.

14-15. (Canceled)

16. (Previously Presented) An apparatus for providing access to resources with the use of personal identification numbers, comprising:

means for concurrently maintaining a system-wide list of resources associated with a plurality of subscribers regardless of subscriber identity and a separate and distinct plurality of lists of resources respectively associated with subscribers;

means for receiving a request from a subscriber to access a resource;

means for first comparing the resource to the system-wide list;

if the resource is included in the system-wide list:

means for providing or denying access to the resource in accordance with the system-wide list;

if the resource is not included in the system-wide list:

means for retrieving one of the plurality of lists associated with the subscriber;

means for next comparing the resource to the retrieved list associated with the subscriber;

means for providing access to the resource if the resource is included in the list associated with the subscriber;

means for requiring the subscriber to input a personal identification number if the resource is not included in the list associated with the subscriber; and

means for providing access to the resource if the subscriber inputs the correct personal identification number.

17. (Original) An apparatus as recited in claim 16 further comprising means for adding the resource to the list associated with the subscriber if the subscriber inputs the correct personal identification number.

18. (Canceled)

19. (Previously presented) An apparatus as recited in claim 16 wherein the system-wide list includes an always deny list, and wherein the means for providing or denying access includes means for denying access to the resource if the resource is included in the always deny list.

20. (Previously presented) An apparatus as recited in claim 16 wherein the system-wide list includes an always require PIN list, and wherein the means for providing or denying access includes means for requiring the subscriber to input a personal identification number if the resource is included in the always require PIN list.

21. (Original) An apparatus as recited in claim 16 wherein the resource is a telephone connection to a destination phone number.

22-23. (Canceled)

24. (Previously presented) An apparatus for providing access to resources with the use of personal identification numbers, comprising:

means for maintaining a first list of resources accessed by a user;

means for maintaining a second list of resources separate from the first list, the second list listing resources to which access is controlled regardless of user identity;

means for first determining whether to allow the user to access resources included in the second list before consulting the resources in the first list;

means for requiring the user to enter a personal identification number to access a further resource not included in the first or second lists; and

means for adding the further resource that the user accesses using the personal identification number to the first list.

25. (Canceled)

26. (Previously Presented) An apparatus as recited in claim 24 wherein the second list includes an always deny list and wherein the first determining means includes means for denying the user access to a still further resource if the still further resource is included in the always deny list.

27. (Previously presented) An apparatus as recited in claim 24 wherein the second list includes an always require PIN list and wherein the first determining means includes means for requiring the user to input a personal identification number to access a still further resource included in the always require PIN list associated with a plurality of users.

28. (Original) An apparatus as recited in claim 24 wherein the resources are telephone connections to destination phone numbers.

29-30. (Canceled)

31. (Previously presented) A method according to claim 1, wherein the system-wide list includes an always allow list containing a phone number associated with emergency services.

32. (Previously presented) A method according to claim 4, wherein the always deny list comprises a phone number associated with fraudulent use.

33. (Previously presented) A method according to claim 5, wherein the always require PIN list comprises a phone number associated with one of an international call and a 900 number call.
34. (Previously presented) A method according to claim 9, wherein the second list includes always allow list containing a phone number associated with emergency services.
35. (Previously presented) A method according to claim 11, wherein the always deny list comprises a phone number associated with fraudulent use.
36. (Previously presented) A method according to claim 12, wherein the always require PIN list comprises a phone number associated with one of an international call and a 900 number call.
37. (Previously presented) An apparatus according to claim 16, wherein the system-wide list includes an always allow list containing a phone number associated with emergency services.
38. (Previously presented) An apparatus according to claim 19, wherein the always deny list comprises a phone number associated with fraudulent use.
39. (Previously presented) An apparatus according to claim 20, wherein the always require PIN list comprises a phone number associated with one of an international call and a 900 number call.
40. (Previously presented) An apparatus according to claim 24, wherein the second list includes an always allow list containing a phone number associated with emergency services.
41. (Previously presented) An apparatus according to claim 26, wherein the always deny list comprises a phone number associated with fraudulent use.
42. (Previously presented) An apparatus according to claim 27, wherein the always require PIN list comprises a phone number associated with one of an international call and a 900 number call.

## EVIDENCE APPENDIX

**None.**

RELATED PROCEEDINGS APPENDIX

**None.**